10337.

Monge, Elaine (SCA)

From: noreply@formstack.com
Sent: Friday, January 20, 2017 9:03 AM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications

Formstack Submission for form Security Breach Notifications

Submitted at 01/20/17 9:02 AM

Business Name:	Hemenway & Barnes LLP
Business Address:	75 State Street 16th Floor Boston, MA 02109
Company Type:	Other
Your Name:	Kurt Somerville
Title:	Managing Partner
Contact Address:	75 State Street 16th Flr Boston, MA 02109
Telephone Number:	(617) 557-9724
Extension:	
Email Address:	ksomerville@hembar.com
Relationship to Org:	Owner
Breach Type:	Electronic
Date Breach was Discovered:	12/07/2016
Number of Massachusetts Residents Affected:	230
Person responsible for data breach.:	3rd Party Provider
Please give a detailed explanation of how the data breach occurred.:	Hemenway & Barnes (the "Firm") was advised by State Street Bank & Trust ("State Street") that an employee of their affiliate had erroneously sent an excel spreadsheet containing account numbers, client names and client addresses to two SEC registered investment advisors who were clients of State Street but did not have rights to this information. We were assured by State Street that both RIA's had destroyed the data upon realizing the data did not belong to them or their clients.

Please select the type of personal information that was included in the breached data.:	Financial Account Numbers = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The breach occurred at the location of a third party service provider. = Selection(s) There is a written contract in place with the third-party provider requiring protection of personal information. = Selection(s)
For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information was restricted to authorized personnel only.:	N/A
Network configuration of breached system:	Closed System
For breaches involving electronic systems, complete the following:	Breached data was encrypted. = Selection(s)
All Massachusetts residents affected by the breach have been notified of the breach.:	Yes
Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::	US Mail = Selection(s)
Date notices were first sent to Massachusetts residents (MM/DD/YYYY):	01/20/2017
All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services .:	No
Law enforcement has been notified of this data breach.:	No
Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.:	We request a thorough explanation from State Street Bank and assurance that the information was not disseminated any further. We have also been assured that State Street Bank has the measures to prevent a similar incident from happening again.

Monge, Elaine (SCA)

From: Hood, Stephanie A. <shood@hembar.com>
Sent: Friday, January 20, 2017 9:09 AM
To: Breaches, Data (SCA)
Cc: Siciliano, John J.; Somerville, Kurt F.
Subject: Report of Data Breach - Notification Sent 1/20/17
Attachments: 4096_001.pdf

Attached is the supporting documentation for the Data Breach Notification entered into your website earlier today. Should you have any questions please do not hesitate to contact me or our Managing Partner, Kurt Somerville. Thank you, Steph

Stephanie A. Hood | Executive Director
Hemenway & Barnes LLP | 75 State Street | Boston, MA 02109 | (617) 557-9770 | e-mail
Website | Hemenway Trust Company

The Official Website of the Office of Consumer Affairs & Business Regulation (OCABR)

Consumer Affairs and Business Regulation

Home > Data Privacy and Security > Data Breach > Data Breach Notifications Submission

Data Breach Notifications Submission

Instructions: Please complete the form below to submit a data breach notification to the Office of Consumer Affairs and Business Regulation. You can also print this submission for your own records. Please note under M.G.L. C93H, a separate notification must be sent to the Attorney General's Office. Please do not include any personally identifiable information for Massachusetts residents in any of the fields.

Section I: Organization & Contact Information

Business Name*
Hemenway & Barnes LLP

Business Address*
75 State Street
16th Floor
Boston (City) Massachusetts (State) 02109 (ZIP Code)

Company Type*
Other ☑

Your Name*
Kurt (First Name) Somerville (Last Name)

Title*
Managing Partner

Contact Address*
75 State Street
16th Flr
Boston (City) Massachusetts (State) 02109 (ZIP Code)

Telephone Number*
(617) 557-9724

Extension

Email Address*
ksomerville@hembar.com

Relationship to Org*
Owner ☑

Section II: Breach Information

Breach Type*
Electronic ☑

Date Breach was Discovered*
12 ☑ 07 ☑ 2016 ☑

Number of Massachusetts Residents Affected*
230

Person responsible for data breach.*
3rd Party Provider ☑

Please give a detailed explanation of how the data breach occurred.*

Hemenway & Barnes (the "Firm") was advised by State Street Bank & Trust ("State Street") that an employee of their affiliate had erroneously sent an excel spreadsheet containing account numbers, client names and client addresses to two SEC registered investment advisors who were clients of State Street but did not have rights to this information. We were assured by State Street that both RIA's had destroyed the data upon realizing the data did not belong to them or their clients.

850/850

Please select the type of personal information that was included in the breached data.*

	Selection(s)
Financial Account Numbers	☑
Social Security Numbers	☐
Driver's License	☐
Credit/Debit Card Number	☐

Please check ALL of the boxes that apply to your breach.*

	Selection(s)
The person(s) with possession of personal information had authorized access	☐
The breach was a result of a malicious/criminal act.	☐
The breach occurred while the data was being transported outside of your premises.	☐
The breach occurred at the location of a third party service provider.	☑
There is a written contract in place with the third-party provider requiring protection of personal information.	☑

Section III: Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data.*

☐ Yes
☐ No
☑ N/A

Physical access to systems containing personal information was restricted to authorized personnel only.*

☐ Yes
☐ No
☑ N/A

Network configuration of breached system*

Closed System ☑

For breaches involving electronic systems, complete the following*

	Selection(s)
Breached data was encrypted.	☑
The key to encrypted data was stolen.	☐
Personal information stored on the breached system was password-protected and/or restricted by user permissions.	☐
N/A	☐

Section IV: Remediation

All Massachusetts residents affected by the breach have been notified of the breach.*

☑ Yes
☐

No

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply):*

	Selection(s)
E-mail	☐
US Mail	☑
Online posting	☐
TV/Radio publication	☐
Other	☐

Date notices were first sent to Massachusetts residents (MM/DD/YYYY)*

01 20 2017

All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services .*

☐ Yes
☑ No

Law enforcement has been notified of this data breach.*

☐ Yes
☑ No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.*

We request a thorough explanation from State Street Bank and assurance that the information was not disseminated any further. We have also been assured that State Street Bank has the measures to prevent a similar incident from happening again.

606/850

**Any documents pertaining to the data breach including the letter being sent to the Massachusetts residents must be sent via email to data.breaches@state.ma.us

Please do not include any personally identifiable information for Massachusetts residents in any email attachment.

Please review the information you have entered and click on the "Submit Form" button below.

Submit Form

Please print this page before submitting.

Print This Page

Did you find the information you were looking for on this page? *

○ Yes
○ No

Send Feedback

STATE STREET.

January 4, 2017

Hemenway & Barnes LLP
75 State Street
Boston, Ma 02109

Dear John,

Inadvertent Data Disclosure
As discussed, State Street was notified by one of our vendors that they inadvertently shared your client account information with two outside independent Registered Investment Advisor firms (RIAs). As part of our internal investigation our vendor has given State Street written confirmation which noted the vendor has contacted the recipient that received the data in error confirming, in an email from the individual recipient, that the data was properly deleted and did not copy or disseminate the email in any way.

As discussed, State Street recently experienced low-risk inadvertent personal data disclosures that affected A number of your customers. The disclosure was caused by a third party vendor error. Since learning of the incident, State Street has diligently worked with the vendor to fully investigate and understand the root cause of the error and to tighten controls and modify procedures to mitigate the risk of recurrence. Based on our investigation and written assurances we have received from the vendor, we believe that the information disclosed in error has been deleted. Below is a summary for the event outlining the relevant facts relative to these efforts.

Incident – Email sent to two RIAs
A State Street vendor BFDS (Boston Financial Data Services), affiliated with State Street and retained to assist State Street with updating its KYC files, sent a spreadsheet via email to two RIAs. The spreadsheet contained information regarding individuals who were not customers of the two RIAs. One of the recipients noticed that the spreadsheet included individuals who were not customers of the RIA and notified BFDS. BFDS immediately contacted the other recipient and confirmed the email and the attachment were deleted and advised State Street.

Investigation:
BFDS provided copies of emails from each of the individuals who received the email confirming that they immediately deleted the email with the attached file. Additionally, State Street contacted the individual recipients and confirmed that they had deleted the email and the attachment and had not saved, copied, forwarded or otherwise disseminated the email or the file.

Cause:
The error occurred because the vendor's employee filtered the spreadsheet by RIA, but did not omit the information that related to other RIAs before attaching the spreadsheet to the email. The error was compounded by the fact that the vendor's employee failed to adhere to procedures that would have caught the error.

Remediation:
BFDS confirmed that it terminated the employee who caused the error and has put in place additional controls and reinforced existing controls. This included (1) requiring a four eyes review of any outgoing email containing personal data, (2) password protecting files emailed to investment managers and (3) when technologically possible, transmitting personal data to investment managers through back-end systems as opposed to email.

Sincerely,

State Street Bank and Trust Company

January __, 2017

Dear _____,

Dear ,

As you know, several years ago Hemenway & Barnes LLP contracted with State Street Bank & Trust Company ("State Street") to provide separate individual custodial accounts for all our clients. Recently, State Street informed us that a State Street subcontractor inadvertently distributed certain of our clients' personal data to two United State based investment advisors for whom State Street also serves as custodian. We immediately demanded that State Street investigate the matter and report back to us. State Street's response is enclosed and confirms that both investment advisors to which this data was sent took appropriate steps to ensure that the data was deleted without further dissemination and not saved or copied.

The data consisted of your name, address and your [H&B/HTC] account number. It did not include social security numbers. Based on State Street's investigation, we are confident that no misuse of the data has occurred or will occur.

We are very sorry that this improper distribution of data took place. State Street has assured us that they have taken corrective action to ensure that your personal data will be safeguarded. We are enclosing consumer protection information concerning data disclosure.

Please let us know if you have any questions.

Sincerely,

Steps You Can Take

You should regularly review your account statements and monitor free credit reports for instances of fraud or identity theft. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions. Under Massachusetts law, you have the right to obtain a police report in regard to this incident. Because this incident did not involve a theft, a police report was not filed. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the Federal Trade Commission (FTC) at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

In addition, you may contact the FTC or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. The FTC encourages those who discover that their information has been misused to file a complaint with the FTC. To do so, or to obtain additional information about identity theft and the steps that you can take to avoid it, you may contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days.

How to Place a Security Freeze on Your Credit Report

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or

permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion by regular, certified, or overnight mail at the addresses below:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.